(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-5448
(P2004-5448A)
(43)公開日　平成16年1月8日(2004.1.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320F	5B017
G06F 1/00	G06F 1/00	370E	5B035
G06K 17/00	G06K 17/00	L	5B058
G06K 19/00	G06K 19/00	T	

審査請求 未請求　請求項の数 10　ＯＬ　（全 14 頁）

(21)出願番号　特願2003-50540 (P2003-50540)
(22)出願日　平成15年2月27日 (2003.2.27)
(31)優先権主張番号　10/086354
(32)優先日　平成14年2月28日 (2002.2.28)
(33)優先権主張国　米国 (US)

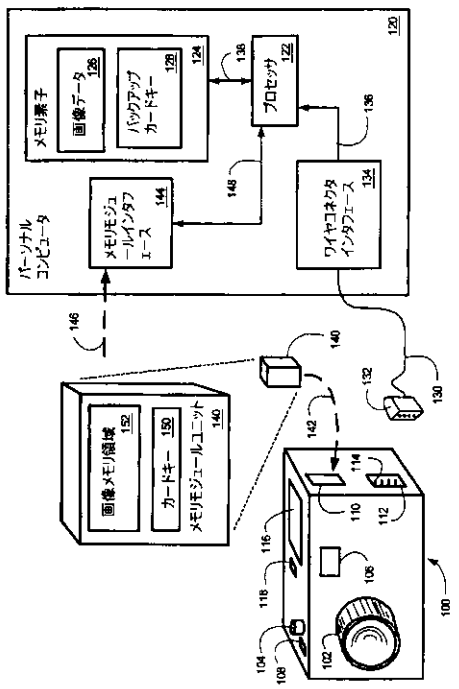
（特許庁注：以下のものは登録商標）
フロッピー
コンパクトフラッシュ

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
ＨＥＷＬＥＴＴ－ＰＡＣＫＡＲＤ　ＣＯＭＰＡＮＹ
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　３０００
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男

最終頁に続く

(54)【発明の名称】カードキーセキュリティシステムおよび方法

(57)【要約】
【課題】電子機器の無許可での使用を防止する
【解決手段】所定のセキュリティコードに対応するセキュリティファイル（２１８）と、電子機器に存在しセキュリティファイル（２１８）を格納するように構成されたメモリ（２１０）と、所定のセキュリティコードに対応しカードキー（１５０）と、カードキー（１５０）をセキュリティファイル（２１８）と比較するように構成されプロセッサ（２０４）と、期間のタイミングをとることにより、その期間が経過した後にプロセッサ（２０４）がカードキーをセキュリティファイルと比較するように構成されたセキュリティタイマ（２２２）とを備えてなるシステム。
【選択図】　図１



【特許請求の範囲】
【請求項１】
所定のセキュリティコードに対応するセキュリティファイルと、
電子機器に存在し前記セキュリティファイルを格納するように構成されたメモリと、
カードキーであって、前記所定のセキュリティコードに対応し、前記電子機器に連結するように構成され、さらに該カードキーを通信するように構成されたポータブルメモリモジュールに存在するカードキーと、
前記カードキーを前記セキュリティファイルと比較するように構成され、通信された前記カードキーを受取るように構成され、さらに前記セキュリティファイルが前記カードキーに対応する場合にのみ前記電子機器の使用を可能にするように構成されたプロセッサと、
期間のタイミングをとることにより、該期間が経過した後に前記プロセッサが前記カードキーを前記セキュリティファイルと比較するように構成されたセキュリティタイマと
を備えてなるシステム。
【請求項２】
前記カードキーは、バックアップカードキーであって第２のメモリに存在しており、該第２のメモリは、該カードキーが該第２のメモリから前記プロセッサに通信されるようにコンピュータに存在するものである、請求項１に記載のシステム。
【請求項３】
前記電子機器は、デジタルカメラ、パーソナルコンピュータ、ラップトップコンピュータおよび個人情報端末からなるグループから選択された少なくともいずれかである請求項２に記載のシステム。
【請求項４】
前記セキュリティタイマは、プロセッサに連結され、前記期間が経過したことを示す信号を該プロセッサに通信するように構成されたハードウェアコンポーネントである、請求項１に記載のシステム。
【請求項５】
電子機器にセキュリティを提供する方法であって、
所定のセキュリティコードに対応するカードキーを受取るステップと、
前記電子機器のメモリのユニットに存在し、前記所定のセキュリティコードに対応するセキュリティキーを受取るステップと、
前記カードキーを前記セキュリティキーと比較するステップと、
前記カードキーが前記セキュリティキーに対応する場合にのみ前記電子機器の使用を可能にするステップと、
前記受取るステップと比較するステップと可能にするステップとが、期間の終結時に実行されるように、該期間のタイミングをとるステップと
を含む方法。
【請求項６】
前記カードキーが前記セキュリティキーに対応しない場合に前記電子機器を使用不可にするステップをさらに含む請求項５に記載の方法。
【請求項７】
前記電子機器は、デジタルカメラ、パーソナルコンピュータ、ラップトップコンピュータおよび個人情報端末からなるグループから選択された少なくともいずれかである、請求項５に記載の方法。
【請求項８】
ユーザに対し前記カードキーを前記電子機器と通信するように促すステップをさらに含む請求項５に記載の方法。
【請求項９】
期間のタイミングをとる前記ステップは、
前記電子機器の起動についてセキュリティタイマに通信するステップと、
前記プロセッサが前記受取るステップと比較するステップと可能にするステップとを実行

するように、期間の終了をプロセッサに通信するステップと
をさらに含むものである、請求項５に記載の方法。
【請求項１０】
前記タイミングをとるステップは、
メモリの第２のユニットに存在するセキュリティタイマロジックをプロセッサにより実行するステップと、
前記期間が経過した時に前記受取るステップと比較するステップと可能にするステップとを開始するステップと
をさらに含むものである、請求項５に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、包括的には、所有物盗難防止テクノロジーに関し、特に、電子機器の無許可な使用を防止するシステムおよび方法に関する。
【０００２】
【従来の技術】
デジタルベースの画像取込装置は、画像をキャプチャーするものである。キャプチャーされた画像または物体の「写真」は、画像取込装置内にあったり、またはそれに連結されたりしているメモリに、デジタルデータフォーマットで格納される。限定されるものではないが、デジタル画像取込装置の例は、静止画像および／またはビデオ画像をキャプチャーするデジタルカメラである。電子機器の多くのタイプと同様に、デジタルカメラは比較的高価である。このため、デジタルカメラは盗難のターゲットになる。
【０００３】
同様に、他の多くの電子機器が盗難のターゲットになる。たとえば、限定されるものではないが、パーソナルコンピュータ（ＰＣ）、ラップトップコンピュータまたは個人情報端末（ＰＤＡ）は、比較的小型で容易に盗まれる電子機器である。
【０００４】
電子機器の所有者は、盗人の手に渡ると電子機器の価値が低下するシステムおよび方法によって利益を得ている。このとき、所有者にとっては電子機器の価値は維持されている。物理的な鍵を使用することにより、その鍵を所有していない盗人の手にある電子機器の価値を低下させることがなされてきた。すなわち、ユーザが有効な鍵を所有していない限り、電子機器は使用不能である。
【０００５】
かかるハードウェア装置は、電子機器のソフトウェアを動作させるためにその電子機器にプラグが差込まれるかまたは連結される。かかるハードウェア装置、または鍵の一例は、「ドングル」として知られる。しかしながら、物理的な鍵および／または他のハードウェア装置は、所有者または許可されたユーザが紛失する可能性のあるものであり、そのため、機器はその物理的な鍵が無ければ動作することができないことにより、所有者に対し価値が喪失しおよび／または重大な不都合をもたらす可能性がある。
【０００６】
さらに、電子機器が物理的な鍵および／または他のハードウェア装置と共に盗まれた場合、その盗人は、電子機器を動作させることができ、おそらくは他人に販売することができるようになる。したがって、物理的な鍵の目的は、盗人もまた鍵を手に入れた場合は無効になる。
【０００７】
【発明が解決しようとする課題】
本発明は、電子機器の無許可での使用を防止するシステムおよび方法を提供することを課題とする。
【０００８】
【課題を解決するための手段】

簡単に説明すると、アーキテクチャにおいて、本システムの一実施形態は、所定のセキュリティコードに対応するセキュリティファイルと、電子機器に存在しセキュリティファイルを格納するように構成されたメモリと、所定のセキュリティコードに対応するカードキーと、カードキーをセキュリティファイルと比較するように構成されたプロセッサと、期間のタイミングをとり、それによってその期間が経過した後にプロセッサがカードキーをセキュリティファイルと比較するように構成されたセキュリティタイマとを備える。さらに、プロセッサは、取得した画像がそのカードキーに対応する場合にのみその電子装置の使用が可能になるように構成される。

【０００９】

図面の構成要素は、必ずしも互いに相対的に一定の比率で縮小されていない。各図面を通して同じ参照番号は対応する部分を示している。

【００１０】

【発明の実施の形態】

本発明は、限定されるものではないが、電子機器、パーソナルコンピュータ（ＰＣ）、デジタルカメラ、ラップトップコンピュータまたは個人情報端末（ＰＤＡ）といった所有物を無許可で使用することを防止するシステムおよび方法を提供する。本発明は、デジタルカメラのメモリモジュールに存在するセキュリティファイルを使用する。セキュリティキーは、カメラの使用を可能にするパスワードとして作用する。本発明の一実施形態は、カードキーをセキュリティファイルと比較するプログラムを実行する。他の装置の中では、特に、カードキーは、メモリモジュールユニットおよび／またはパーソナルコンピュータに格納されてよい。所有物にカードキーが提供されていない場合、所有物の無許可の使用を防止するシステムは、その所有物を使用不可にする。

【００１１】

本発明のコンポーネント、動作および機能性を教示する便宜上、本発明を、デジタルカメラ１００（図１）で実施されるものとしてまたはその一部であるものとして説明する。本発明の一実施形態は、限定されないがメモリ媒体等のモジュール式の挿入可能コンポーネントと動作するように構成された任意の電子機器において等しく適用可能である。たとえば、限定されないが、メモリ媒体に連結するかまたはそれを収容するように構成された、パーソナルコンピュータ、ラップトップコンピュータまたは個人情報端末（ＰＤＡ）は、本発明の代替実施形態である。たとえば、一実施形態は、限定されないが、フロッピーディスク、コンパクトディスク（ＣＤ）、コンパクトフラッシュ（ＣＦ）カード、パーソナルコンピュータカード、ミニコンパクトディスク等のメモリモジュールに連結するかまたはそれを収容するように構成された、パーソナルコンピュータとして実施される。このため、本発明は、かかるいかなるタイプの電子機器とも動作するように組み込まれる。

【００１２】

図１は、デジタルカメラ１００の無許可な使用を防止するシステムを有する、本発明によるデジタルカメラシステムのブロック図である。デジタルカメラ１００は、さらに、少なくともレンズユニット１０２と、画像取込作動ボタン１０４と、ビューレンズ１０６と、電源スイッチ１０８と、メモリユニットインタフェース１１０と、プラグインインタフェースユニット１１２とを含む。一実施形態では、プラグインインタフェースユニット１１２は、複数の接続ピン１１４を含む。ディスプレイ１１６は、キャプチャーする前に画像をプレビューするためかまたはキャプチャーした画像を見るために使用される。例示の便宜上、ディスプレイ１１６は、デジタルカメラ１００の上部に示す。

【００１３】

デジタルカメラ１００の動作は、電源スイッチ１０８かまたは同じ機能性を有する等価な装置の作動によって開始する。デジタルカメラ１００がオンとなった時、ディスプレイ１１６は、通常は、デジタルカメラ１００の限られたバッテリ電力を節約するためにオフのままである。限定されないが制御ボタン１１８等の適当なコントローラ装置の作動により、ディスプレイ１１６がオンとなり、それによってデジタルカメラ１００のユーザ（図示せず）はレンズユニット１０２を通して検出された画像を見ることができる。代替的に、

前にキャプチャーされた画像またはメニュー画面の画像が最初に表示されてもよい。代替実施形態では、作動されると、さらに他のボタン、スイッチまたは制御インタフェース装置がディスプレイ１１６をオンにするように構成される。

【００１４】

レンズユニット１０２は、画像の焦点合せに使用される既知の装置である。操作者は、キャプチャーされる画像に焦点を合わせ、デジタルカメラ１００によってキャプチャーされる画像の性質に満足すると、画像取込作動ボタン１０４（シャッタボタンまたはシャッタリリースボタンとも呼ばれる）を作動することにより、デジタルカメラ１００がデジタル画像を記録するようにし、それによって画像を「撮影する」。デジタルカメラ１００の操作者は、ディスプレイ１１６に画像をキャプチャーする前に画像を視覚的にプレビューしてよくおよび／またはビューレンズ１０６を通して直接画像を見ることができる。

【００１５】

図１は、さらに、デジタルカメラ１００によってキャプチャーされたデジタル画像を、取出し、処理し、プリントしかつ／または電子メールで送信することができるように、一般にデジタルカメラと共に使用されるパーソナルコンピュータ１２０を示す。パーソナルコンピュータ１２０は、少なくとも１つのプロセッサ１２２とメモリ素子１２４とを含む。メモリ素子１２４は、さらに、少なくとも画像データ領域１２６とバックアップカードキー１２８とを含む。デジタルカメラ１００から取出された画像データは、画像データ領域１２６に格納される。バックアップカードキー１２８は、英数字、または二進数、十六進数若しくは同様のコード体系等の他の適当なコードによる文字列に対応している、パスワード、セキュリティコード、個人識別コード（ｐｅｒｓｏｎａｌ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｃｏｄｅ（ＰＩＮ））、あるいは、他の適当識別子として機能するように構成された、格納されたデータである。

【００１６】

一実施形態では、デジタルカメラ１００は、接続１３０を介してパーソナルコンピュータ１２０にキャプチャーした画像を転送する。接続１３０は、限定されないがユニバーサルシリアルバス（ＵＳＢ）、シリアル、パラレル接続等、いかなる適当なコネクタであってもよい。代替的に、限定されないが無線周波数および赤外線等、無線転送媒体を採用することができる。ハードワイヤ接続を採用する一実施形態では、接続１３０は、プラグインアタッチメント１３２または他の適当な連結装置に連結される。プラグインアタッチメント１３２は、プラグインインタフェースユニット１１２と嵌合するように構成される。パーソナルコンピュータ１２０およびデジタルカメラ１００のユーザは、単にプラグインアタッチメント１３２をプラグインインタフェース１２０に嵌合することにより、デジタルカメラ１００とパーソナルコンピュータ１２０との間の接続性を確立する。ユーザは、パーソナルコンピュータ１２０および／またはデジタルカメラ１００の例示的な実施形態に対し、デジタル画像が、デジタルカメラ１００からワイヤコネクタインタフェース１３４、接続１３６、プロセッサ１２２、接続１３８を通してメモリ１３０の画像データ領域１２６まで転送されるようにするロジックを実行させるように指示する。

【００１７】

デジタルカメラ１００の実施形態では、デジタル画像データはメモリモジュールユニット１４０に格納される。デジタルカメラ１００で画像をキャプチャーする場合、破線１４２で表される挿入の経路によって示すように、メモリモジュールユニット１４０は、メモリユニットインタフェース１１０を通してデジタルカメラ１００に連結される。メモリモジュールユニット１４０は、限定されないが、標準コンピュータディスク、フロッピーディスク、コンパクトディスク（ＣＤ）、ミニコンパクトディスクまたは他の適当なメモリ媒体等、様々な方法でフォーマットされてよい。メモリモジュールユニット１４０をメモリ媒体としてフォーマットすることにより、パーソナルコンピュータ１２０との単純なインタフェースが可能になる。

【００１８】

デジタル画像データは、破線１４６によって表す挿入の経路によって示すように、メモリ

モジュールユニット１４０をデジタルカメラ１００から取外し、メモリモジュールインタフェース１４４に連結することにより、パーソナルコンピュータ１２０に転送される。通常、メモリモジュールユニット１４０が直接パーソナルコンピュータ１２０に連結されるように、パーソナルコンピュータ１２０の表面に、都合のよい連結ポートまたはインタフェース（図示せず）が設けられる。メモリモジュールユニット１４０がパーソナルコンピュータ１２０に連結されると、デジタル画像データは、メモリモジュールインタフェース１４４、接続１４８、プロセッサ１２２、接続１３８を介してメモリ素子１２４の画像データ領域１２６に転送される。

【００１９】

便宜上、デジタルカメラ１００を、物理コネクタに連結されるように構成されたプラグインインタフェース１２０と、メモリモジュールユニット１４０を収容するように構成されたメモリユニットインタフェース１１０との両方を採用するものとして示す。デジタルカメラ１００の他の実施形態は、キャプチャーした画像のパーソナルコンピュータ１２０への転送を容易にするために、プラグインインタフェース１１２かまたはメモリユニットインタフェース１１０のいずれかを採用する。

【００２０】

便宜上、パーソナルコンピュータ１２０を、当該選択されたコンポーネントのみを有するように示す。しかしながら、パーソナルコンピュータ１２０は、図１に示さない追加の内部コンポーネントを含む。デジタルカメラ１００もまた、図１に示さない追加のコンポーネントを含む。

【００２１】

一実施形態では、メモリモジュールユニット１４０は、カードキー１５０と画像メモリ領域１５２とを有する。好ましくは、カードキー１５０は、隠しファイルおよび／または保護ファイルである。したがって、許可されていない人にとっては、カードキー１５０のコピーを容易に作成することができない。

【００２２】

デジタルカメラ１００を使用する前に、パーソナルコンピュータ１２０にメモリモジュールユニット１４０が連結される。ユーザは、カードキー１５０とバックアップカードキー１２８とに格納される秘密コードを選択する。上述したように、この秘密コードは、パスワード、セキュリティコード、個人識別コード（ＰＩＮ）または他の適当な識別子として機能するように構成される。ユーザが、秘密コードを選択しそれをパーソナルコンピュータ１２０に伝えると、プロセッサ１２２は、秘密コードをバックアップカードキー１２８としてメモリ素子１２４に格納し、またその秘密コードを、カードキー１５０として格納するためにメモリモジュールインタフェース１４４を介してメモリモジュールユニット１４０に通信する。カードキー１５０は、概して、隠しおよび／または保護ファイルとして格納され、それによって別のメモリモジュールユニット１４０への転送が防止される。一実施形態は、限定されないが、シリアル番号または製造日等、メモリモジュールユニット１４０に一意かつ特定の情報を含み、それによってカードキー１５０はメモリモジュールユニット１４０に対して固有のものになる。したがって、カードキー１５０を、異なるメモリモジュールユニット１４０にコピーすることはできない。デジタルカメラ１００と共に提供され、パーソナルコンピュータ１２０と共に提供されかつ／または別々に提供されるコンピュータソフトウェアに、カードキー１５０およびバックアップカードキー１２８を作成するソフトウェアを含めることができる。

【００２３】

ユーザが、メモリモジュールユニット１４０をデジタルカメラ１００に連結すると、デジタルカメラ１００は、後により詳細に説明するように、カードキー１５０をセキュリティファイル２１８と比較することにより、デジタルカメラ１００を使用しようと試みる人が許可されたユーザであるか否かを判断する。メモリモジュールユニットがデジタルカメラ１００に連結されていない場合、あるいはカードキー１５０が許可されたセキュリティコードに対応していない場合、デジタルカメラ１００は使用不可となり、作動しない。

【００２４】
したがって、本発明を採用するデジタルカメラ１００の実施形態は、キャプチャーされた画像データをメモリモジュールユニット１４０に格納するように構成される。このため、カードキー１５０は、盗人または他の無許可のユーザからは不可視であり、容易に検出されることもない。かかる盗人かまたは他の無許可のユーザは、デジタルカメラ１００を使用するためにデジタルカメラ１００とメモリモジュールユニット１４０との両方にアクセスする必要がある。したがって、盗人は、デジタルカメラ１００を起動するためにデジタルカメラ１００にメモリモジュールユニット１４０を連結しなければならない、ということを知らなければならない。そのため、デジタルカメラ１００は、本発明によって動作不能とされ、盗人または他の無許可のユーザには殆どまたはまったく価値が無く、したがって望ましいものでなくなる。

【００２５】
図２は、デジタルカメラ１００の実施形態のブロック図である。切取内部線２０２は、デジタルカメラ１００の外面に存在するコンポーネントとデジタルカメラ１００の内部に存在するコンポーネントとの境界を示している。このため、制御ボタン１１８、レンズユニット１０２、画像取込作動ボタン１０４、電源スイッチ１０８、メモリユニットインタフェース１１０、プラグインインタフェース１２０およびディスプレイ１１６は、デジタルカメラ１００の表面に存在するコンポーネントとして認識される。

【００２６】
デジタルカメラ１００の内部コンポーネントは、少なくともカメラプロセッサ２０４と、フォトセンサ２０６と、メモリ記憶部インタフェース２０８と、メモリ２１０とを含む。メモリ２１０はさらに、データ管理ロジック２１２と、カメラ画像データ領域２１４と、画像ディスプレイ制御ロジック２１６と、セキュリティファイル２１８と、カードキーセキュリティシステム２２０とを含む。本発明によるデジタルカメラの代替実施形態は、後により詳細に説明するセキュリティタイマ２２２を含む。

【００２７】
デジタルカメラ１００は、カードキー１５０から情報をコピーすることによりセキュリティファイル２１８を作成する。したがって、カードキー１５０を有するメモリモジュールユニット１４０が、デジタルカメラ１００に連結される。カメラプロセッサ２０４は、接続２２４を介してカードキー１５０を呼び出し、それを、接続２２６を介して、メモリ素子２１０に存在するセキュリティファイル２１８に保存する。

【００２８】
他の実施形態では、デジタルカメラ１００は、パーソナルコンピュータ１２０からバックアップカードキー１２８を呼び出す。このため、デジタルカメラ１００がパーソナルコンピュータ１２０に連結されると、バックアップカードキー１２８が、プラグインインタフェースユニット１１２において受取られ、その後、接続２２８を介してカメラプロセッサ２０４に通信される。

【００２９】
一実施形態では、カードキー１５０は、デジタルカメラ１００の所有者のパーソナルコンピュータ等、単一の指定された装置に提供される情報からのみ作成される。このため、盗人かまたは盗人からデジタルカメラ１００を購入する人は、カードキー１５０を作成することができない。したがって、本発明により、デジタルカメラは使用不可のままになる。

【００３０】
また、デジタルカメラシステムは、カードキー１５０が作成されるプロセスと同じプロセスによってセキュリティファイル２１８を作成することも可能である。ユーザは、デジタルカメラ１００を最初に使用する時にセキュリティファイル２１８を作成するように促され得る。他の実施形態では、ユーザに対し、カードキーセキュリティシステム２２０の起動時にセキュリティファイル２１８を作成または置換するように促してもよい。他の実施形態では、ユーザがセキュリティファイル２１８を置換したい場合、既存のカードキー１５０を提供するようにユーザに要求してよい。

【００３１】
本発明によるカードキーセキュリティシステム２２０は、ソフトウェア（たとえば、ファームウェア）、ハードウェアまたはそれらの組合せで実施することができる。一実施形態では、カードキーセキュリティシステム２２０は、実行可能プログラムとしてソフトウェアで実施され、カメラプロセッサ２０４によって実行される。カメラプロセッサ２０４は、ソフトウェア、特にメモリ素子２１０に格納されたソフトウェアを実行する適当なハードウェア装置である。カメラプロセッサ２０４は、いかなる適当なカスタムメイドまたは市販のプロセッサともすることができる。
【００３２】
メモリ素子２１０は、揮発性メモリ素子（たとえば、ランダムアクセスメモリ（ＤＲＡＭ、ＳＲＡＭ、ＳＤＲＡＭ等のＲＡＭ））と不揮発性メモリ素子（たとえば、ＦＬＡＳＨ、ＲＯＭ、ハードドライブ、テープ、ＣＤＲＯＭ等）とのうちの任意の１つまたは組合せを含むことができる。さらに、メモリ素子２１０は、電子、磁気、光および／または他のタイプの記憶媒体を組込んでよい。なお、メモリ素子２１０は、分散アーキテクチャを有することができ、その場合、あらゆるコンポーネントが互いからリモートに配置されるが、カメラプロセッサ２０４はそれらにアクセスすることができる。
【００３３】
メモリ素子２１０のソフトウェアは、各々が論理機能を実現する実行可能命令の順序付きリストを有する１つまたは複数の別々のプログラムを含んでよい。図１の実施例では、メモリ素子２１０のソフトウェアは、本発明によるカードキーセキュリティシステム２２０とデータ管理ロジック２１２とを含む。一実施形態では、データ管理ロジック２１２は、カードキーセキュリティシステム２２０等の他のコンピュータプログラムの実行を制御し、スケジューリングと、入出力制御と、ファイルおよびデータ管理と、メモリ管理と、通信制御および関連サービスとを提供する。
【００３４】
一実施形態では、カードキーセキュリティシステム２２０は、ソースプログラム、実行可能プログラム（オブジェクトコード）、スクリプト、または実行される命令のセットを含む任意の他のエンティティである。ソースプログラムである場合、そのプログラムは、データ管理ロジック２１２に関して適当に動作するように、メモリ素子２１０に含まれても含まれなくてもよいコンパイラ、アセンブラ、インタプリタ等を介して変換される。さらに、カードキーセキュリティシステム２２０を、（ａ）データのクラスおよびメソッドを有するオブジェクト指向プログラミング言語かまたは（ｂ）ルーチン、サブルーチンおよび／または関数を有する、例えば限定されないがＣ、Ｃ＋＋、Ｐａｓｃａｌ、Ｂａｓｉｃ、Ｆｏｒｔｒａｎ、Ｃｏｂｏｌ、Ｐｅｒｌ、ＪａｖａおよびＡｄａ等の手続きプログラミング言語として書くことができる。一実施形態では、カードキーセキュリティシステム２２０は、ＣまたはＣ＋＋言語で実施される。
【００３５】
デジタルカメラ１００が動作中である時、カメラプロセッサ２０４は、メモリ素子２１０内に格納されたソフトウェアを実行し、メモリ素子２１０との間でデータを通信し、概してソフトウェアに準ずるデジタルカメラ１００の動作を制御するように構成される。カードキーセキュリティシステム２２０およびデータ管理ロジック２１２は、全体としてまたは部分的に読み出され、その後カメラプロセッサ２０４によって実行される。
【００３６】
カードキーセキュリティシステム２２０は、図１に示すようなソフトウェアで実施される場合、任意のコンピュータ関連システムまたは方法によるかまたはそれと関連して使用するために、任意の適当なコンピュータ読取可能媒体に格納することができる。この文書のコンテキストにおいては、コンピュータ読取可能媒体とは、コンピュータ関連システムまたは方法によるかまたはそれと関連して使用されるコンピュータプログラムを内蔵するかまたは格納することができる、電子、磁気、光あるいは他の物理装置または手段である。カードキーセキュリティシステム２２０を、コンピュータベースシステム、プロセッサ内

蔵システム、あるいは命令実行システム、装置または機器からの命令をフェッチしそれら命令を実行することができる他のシステム等の、命令実行システム、機器または装置によるかまたはそれと関連して使用されるために、任意のコンピュータ読取可能媒体において具体化することができる。本文書のコンテキストにおいては、「コンピュータ読取可能媒体」とは、命令実行システム、機器または装置によるかまたはそれに関連して使用されるプログラムを格納し、通信し、伝播し、または移送することができるいかなる手段ともすることができる。コンピュータ読取可能媒体は、たとえば、限定されないが、電子、磁気、光、電磁気、赤外線または半導体のシステム、機器、装置または伝播媒体とすることができる。コンピュータ読取可能媒体のより特定の例（非網羅的リスト）には、以下のものが含まれる。すなわち、１つまたは複数のワイヤを有する電気的接続（電子）、ポータブルコンピュータディスケット（磁気、コンパクトフラッシュカード、セキュアデジタルカード等）、フラッシュメモリ、ランダムアクセスメモリ（ＲＡＭ）（電子）、リードオンリメモリ（ＲＯＭ）（電子）、消去可能プログラム可能リードオンリメモリ（ＥＰＲＯＭ、ＥＥＰＲＯＭまたはフラッシュメモリ）（電子）、光ファイバ（光）およびポータブルコンパクトディスクリードオンリメモリ（ＣＤＲＯＭ）（光）が含まれる。

【００３７】

代替実施形態では、カードキーセキュリティシステム２２０は、ハードウェアで実現される場合、以下のテクノロジーのうちの任意のものかまたは組合せにより実施することができる。すなわち、データ信号に対して論理機能を実現する論理ゲートを有するディスクリート論理回路（複数可）、適当な組合せ論理ゲートを有する特定用途向け集積回路（ＡＳＩＣ）、プログラマブルゲートアレイ（複数可）（ＰＧＡ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）等である。

【００３８】

デジタルカメラ１００の一実施形態は、セキュリティタイマ２２２を含む。後により詳細に説明するように、セキュリティタイマ２２２は、所定期間タイミングをとることにより、デジタルカメラ１００が起動後にその期間の間起動するようにする。この期間は、少なくとも、セキュリティファイル２１８をカードキー１５０（図１）と比較するプロセスに対して十分である。一実施形態では、セキュリティタイマ２２２は、上述した期間のタイミングをとるように構成された物理装置である。したがって、期間のタイミングを示す適当な信号が、接続２３０を介してカメラプロセッサ２０４に提供される。

【００３９】

一実施形態では、上述した期間は固定されている。さらに別の実施形態では、期間は調整可能である。したがって、ユーザが期間を調整することができるように、セキュリティタイマ２２２に接続２３４を介して連結された期間アジャスタ２３２が設けられる。期間アジャスタ２３２は、限定されないがダイアル、時間をインクリメントする１つまたは複数のタッチセンシティブプッシュボタン、またはタッチセンシティブ表示画面等、いかなる適当な物理装置であってもよい。他の実施形態では、期間が調整可能であるように、カードキーセキュリティシステム２２０の一部としてソフトウェアが設けられる。したがって、適当な制御信号をセキュリティタイマ２２２に提供することにより、期間が電子的に調整される。さらに他の実施形態では、期間アジャスタ２３２は、プロセッサ２０４または他の適当なコンポーネントに連結される。

【００４０】

他の実施形態では、セキュリティタイマ２２２は、カードキーセキュリティシステム２２０の一部として含まれるソフトウェアとして実施される。このため、上述した期間のタイミングをとるために、カメラプロセッサ２０４に存在するクロック等、デジタルカメラ１００内の内部クロックが採用される。

【００４１】

セキュリティタイマ２２２を採用する本発明によれば、カードキーセキュリティシステム２２０がセキュリティファイル２１８をカードキー１５０と比較した後、デジタルカメラが動作することが可能になる。このため、フォトセンサ２０６にキャプチャーされた画像

は、接続２３６を介してカメラプロセッサ２０４に通信される。

【００４２】

デジタルカメラ１００が、キャプチャーした画像をカメラ画像データ領域２１４に保存するように構成されている場合、カメラプロセッサ２０４は、キャプチャーされた画像をカメラ画像データ領域２１４に格納する。メモリモジュールユニット１４０に存在する画像メモリ領域１５２を採用するデジタルカメラの実施形態では、キャプチャーされた画像は、接続２２４を介して画像メモリ領域１５２に通信され保存される。実施形態によっては、キャプチャーされた画像が画像メモリ領域１５２に格納するために適したデータに変換されるように、メモリ記憶部インタフェース２０８が接続２２４の途中に含まれる。

【００４３】

一実施形態では、デジタルカメラ１００は、セキュリティファイル２１８をカードキー１５０から識別することができるように、時刻または他の適当な時間ベースのマーカをセキュリティファイル２１８と関連付ける。時刻または他の適当な時間ベースのマーカの限定されない実施例には、何分間、何時間、何日、何週間、特定の日付および／または特定の時刻等が含まれる。デジタルカメラ１００は、指定された期間および／またはマーカを監視し、期間および／またはマーカの終了時に、デジタルカメラ１００のユーザに対しカードキー１５０を提供するように促す。したがって、デジタルカメラ１００が使用可能であり続ける場合、カードキー１５０を提供しなければならない。カードキー１５０を提供しないことにより、カードキーセキュリティシステム２２０がデジタルカメラ１００を使用不可にする。

【００４４】

たとえば、限定されないが、デジタルカメラ１００の所有者は、１月１日から１月１０日まで１０日間の休暇で出かけるものとする。所有者は、セキュリティタイマ２２２をセットすることによるかまたはセキュリティファイル２１８で時刻または他の適当な時間ベースマーカを指定することにより、デジタルカメラ１００が作動状態であり続ける１０日間の（またはそれより長い）期間を指定してよい。１０日間の最後に、デジタルカメラ１００のユーザは、デジタルカメラ１００が作動状態であり続けるようにカードキー１５０を提供しなければならない。このため、デジタルカメラ１００は、盗難された場合、１０日間の後に使用不可になる。代替的に、所有者は、１月１０日にまたはその直後に、デジタルカメラ１００がカードキー１５０の提供をユーザに促すように指定してよい。このように、デジタルカメラ１００は、盗難された場合、１月１０日という指定された日付の後に使用不可になる。

【００４５】

図３は、カードキーセキュリティシステム２２０（図２）の実施形態のフローチャート３００である。フローチャート３００は、カードキーセキュリティシステム２２０の可能な実施のアーキテクチャ、機能性および動作を示す。これに関し、各ブロックは、指定された論理機能（複数可）を実施する１つまたは複数の実行可能命令を含む、モジュール、セグメントまたはコードの一部を表す。また、代替実施態様によっては、ブロックに示す機能は、フローチャート３００に示す順序以外の順序で行われてよい。たとえば、下でさらに明確にするように、フローチャート３００に連続して示す２つのブロックは、実際には、実質的に同時に実行されてよく、あるいは、ブロックは時に、含まれる機能性によって逆の順序に実行されてもよい。

【００４６】

ブロック３０２において、カードキーセキュリティシステム２２０が起動される。一実施形態では、カードキーセキュリティシステム２２０は、デジタルカメラ１００がオンとされる時はいつも起動される。他の実施形態では、ユーザがカードキーセキュリティシステム２２０をマニュアルでオンとする時に、カードキーセキュリティシステム２２０が起動される。ユーザは、データ管理ロジック２１２に関連する起動ロジックを介してカードキーセキュリティシステム２２０をオンとしてよい。起動は、ディスプレイ１１６に示すメニューシステムを介して行われてよい。

【００４７】
ブロック３０４において、カードキーセキュリティシステム２２０は、セキュリティタイマ２２２がセットされたか否かを判断する。ブロック３０４においてセキュリティタイマ２２２がセットされている場合（ＹＥＳ条件）、カードキーセキュリティシステム２２０により、デジタルカメラ１００は所定期間動作することができる。期間の最後に、ユーザは、カードキー１５０を提供するように要求される。したがって、セキュリティタイマ２２２は、起動時にこの期間を追跡する。カードキーセキュリティシステム２５２が、セキュリティタイマ２２２がセットされなかったと判断した場合、プロセスはブロック３０６に進む。すなわち、セキュリティタイマ２２２がセットされなかった場合（ＮＯ条件）、デジタルカメラ１００は、直ちにユーザに対しカードキー１５０を提供するよう促す。

【００４８】
カードキーセキュリティシステム２２０が、セキュリティタイマ２２２がセットされていると判断した場合（ＹＥＳ条件）、プロセスはブロック３０８に進む。ブロック３０８において、カードキーセキュリティシステム２２０は、セキュリティタイマにセットされた時間が満了したか否かを判断する。時間が満了していない場合（ＮＯ条件）、プロセスはブロック３１０に進み、デジタルカメラ１００を使用可能にする。そして、プロセスはブロック３１２に進み、時間をインクリメントする。ブロック３０８、３１０および３１２の論理ループは、期間の満了まで繰返される。期間が満了すると、プロセスはブロック３０６に進む。

【００４９】
ブロック３０６において、カードキーセキュリティシステム２２０は、ユーザに対してカードキーを提供するよう促す。カードキー１５０は、メモリモジュールユニット１４０に存在する。したがって、上述したようにメモリモジュールユニットがデジタルカメラに連結され、それによってカードキー１５０が提供される。ブロック３１４において、カードキーセキュリティシステム２２０は、メモリユニットインタフェース１１０を介してメモリモジュールユニット１４０からカードキー１５０を取出す。

【００５０】
代替的に、パーソナルコンピュータ１２０に関連しメモリ素子１２４に格納されるバックアップカードキー１２８が提供されてよい。したがって、デジタルカメラ１００は、上述したようにパーソナルコンピュータ１２０に連結される。バックアップカードキー１２８は、パーソナルコンピュータ１２０からカメラプロセッサ２０４に通信される。

【００５１】
ブロック３１６において、カードキーセキュリティシステム２２０は、セキュリティファイル２１８がカードキー１５０、または代替的にバックアップカードキー１２８と等価であるか否かを判断する。任意の適当な比較アルゴリズムが、比較を実行してよい。カードキー１５０がセキュリティファイル２１８と等価であるかそれに対応する場合（ＹＥＳ条件）、プロセスはブロック３１８に進み、デジタルカメラ１００を使用可能にする。カードキーセキュリティシステム２２０が、カードキー１５０がセキュリティファイル２１８と等価でないかまたはそれに対応しないと判断した場合（ＮＯ条件）、プロセスはブロック３２０に進む。ブロック３２０において、カードキーセキュリティシステム２２０は、デジタルカメラ１００を使用不可にする。

【００５２】
他の実施形態では、カードキーセキュリティシステム２２０は、所有者のパーソナルコンピュータを介して使用不可にされてよい。デジタルカメラ１００は、上述したように、接続１３０を介してパーソナルコンピュータ１２０に連結される。デジタルカメラ１００に接続１３０を介して適当な信号が提供されることにより、カードキーセキュリティシステム２２０が、デジタルカメラ１００が起動するべきでないと認識する。したがって、デジタルカメラ１００は、カードキー１５０が無い場合使用不可になる。代替的に、メモリモジュールユニット１４０に適当な信号が提供される。その適当な信号は、特別なカードキー１５０として格納されるかまたはメモリモジュールユニット１４０の別の場所に格納さ

れてよく、メモリモジュールユニット１４０がメモリユニットインタフェース１１０に連結された場合に、デジタルカメラ１００によって受取られる。

【００５３】

図４は、カードキーセキュリティシステム２２０とセキュリティファイル２１８とを格納するメモリ素子２１０を含む、デジタルカメラ４００で実施される本発明によるカードキーセキュリティシステム２２０の代替実施形態のブロック図である。デジタルカメラ４００は、セキュリティタイマ２２２（図２）もセキュリティタイマロジックも使用しない。起動時、デジタルカメラ４００を、上述したように、カードキー１５０を有するメモリモジュールユニット１４０に連結しなければならない。あるいは、デジタルカメラ４００を、上述したように、バックアップカードキー１２８を有するパーソナルコンピュータ１２０に連結しなければならない。セキュリティファイル２１８がカードキー１５０（またはバックアップカードキー１２８）に対応するかまたはそれと等価である場合、カードキーセキュリティシステム２２０はカメラ４００を使用可能にする。カードキーセキュリティシステム２２０が、セキュリティファイル２１８がカードキー１５０（またはバックアップカードキー１２８）と等価でないと判断した場合、カードキーセキュリティシステム２２０は、カメラ４００を使用不可にする。

【００５４】

カードキーセキュリティシステム２２０の他の実施形態は、セキュリティファイル２１８が存在しない場合であってもデジタルカメラ１００を使用可能にするロジックを含む。たとえば、一実施形態では、デジタルカメラ１００は、最初に製造業者、卸業者または再販売業者から取得された時に使用不可にされる。真正の購入者等、許可されたユーザは、パーソナルコンピュータ１２０のメモリ素子１２４に特別なキーをロードする。かかる特別なキーは、最初、便宜上バックアップカードキー１２８かまたはメモリ素子１２４の他の適当なロケーションに存在してよい。特別なキーは、永久的であっても一時的であってもよい。一時的なものである場合、バックアップキーが上述したように定義される時に置換される。

【００５５】

ユーザが最初にデジタルカメラ１００を使用する時、デジタルカメラ１００がパーソナルコンピュータ１２０に連結された場合、特別なキーは接続１３０を介して受取られる。代替的に、特別なキーは、上述したようにメモリモジュールユニット１４０内に配置されてよい。したがって、実施形態により、デジタルカメラ１００が最初に起動され、上述したように新たなカードキーセキュリティシステム２２０を作成することができる。さらに、カードキー１５０が紛失されるかまたは破壊された場合、デジタルカメラ１００を再起動することにより、新たなおよび／または置換カードキー１５０が定義される。

【００５６】

本発明の上述した実施形態、特に任意の「好ましい」実施形態は、単に本発明の原理を明確に理解するために示された、単に実施の可能な実施例である、ということを強調しなければならない。本発明の精神および原理から実質的に逸脱することなく、本発明の上述した実施形態（複数可）に対し、多くの変形および変更がなされてよい。かかる変更および変形は、この開示および本発明の範囲内に含まれ上述した特許請求の範囲によって保護されることが意図されている。

【図面の簡単な説明】

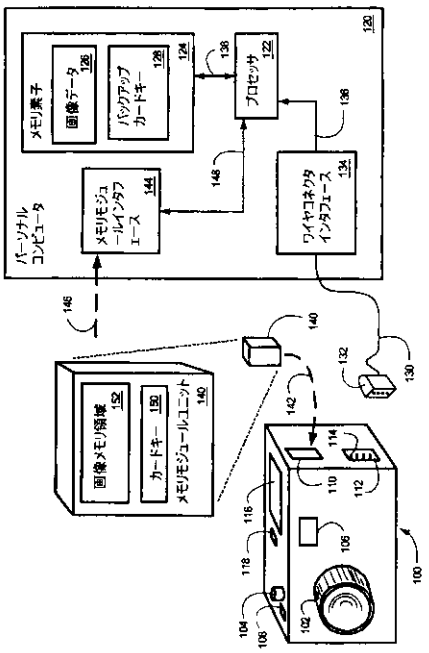
【図１】デジタルカメラ、パーソナルコンピュータおよびメモリカードを含む、本発明によるデジタルカメラシステムの実施形態のブロック図である。

【図２】本発明による、カードキーセキュリティシステムを格納するメモリ素子とセキュリティタイマとを有する図１のデジタルカメラの実施形態のブロック図である。

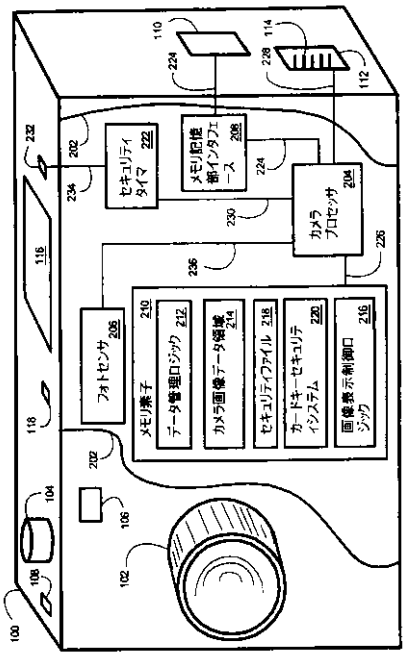
【図３】図２のカードキーセキュリティシステムの実施形態のフローチャートである。

【図４】本発明による、カードキーセキュリティシステムを格納するメモリ素子を有する図１のデジタルカメラの実施形態のブロック図である。

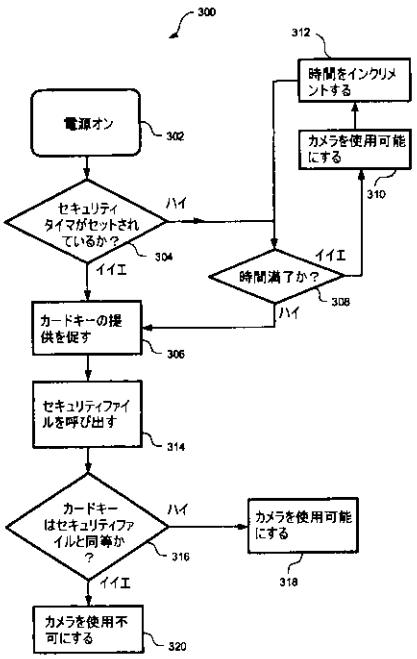
【図１】


パーソナルコンピュータ
メモリ素子
画像データ
バックアップカードキー
プロセッサ
メモリモジュールインタフェース
ワイヤコネクタインタフェース
メモリモジュールユニット
画像メモリ領域
カードキー

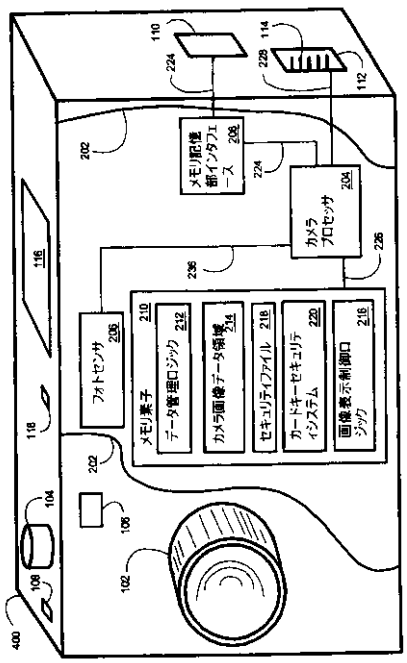
【図２】


メモリ素子
データ管理ロジック
カメラ画像データ領域
セキュリティファイル
カードキーセキュリティシステム
画像表示制御ロジック
フォトセンサ
セキュリティタイマ
メモリ記憶部インタフェース
カメラプロセッサ

【図３】


電源オン
セキュリティタイマがセットされているか？
ハイ
イイエ
時間満了か？
時間をインクリメントする
カメラを使用可能にする
カードキーの提供を促す
セキュリティファイルを呼び出す
カードキーはセキュリティファイルと同等か？
カメラを使用可能にする
カメラを使用不可にする

【図４】


メモリ素子
データ管理ロジック
カメラ画像データ領域
セキュリティファイル
カードキーセキュリティシステム
画像表示制御ロジック
フォトセンサ
メモリ記憶部インタフェース
カメラプロセッサ

フロントページの続き

(72)発明者　マーク・ネルソン・ロビンス
アメリカ合衆国コロラド州８０６３１，グリーリー，サーティーンス・ストリート　１４２５
(72)発明者　ヘザー・ノエル・ビーン
アメリカ合衆国コロラド州８０５２１，フォート・コリンズ，ノース・ウィットコム・ストリート
２１４

Ｆターム(参考) 5B017 AA03 BA05 BB10
5B035 BB09 BC00
5B058 CA01 YA13 YA20